

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2005 年 7 月 14 日 (14.07.2005)

PCT

(10) 国際公開番号  
WO 2005/064485 A1

(51) 国際特許分類: G06F 15/00, 1/00

(21) 国際出願番号: PCT/JP2003/016815

(22) 国際出願日: 2003 年 12 月 25 日 (25.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三井物産株式会社 (MITSUI & CO., LTD.) [JP/JP]; 〒100-0004 東京都千代田区大手町一丁目 2 番 1 号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 大島 俊一 (OSHIMA, Shunichi) [JP/JP]; 〒270-0176 千葉県流山市加 3-6-1 四番館 905 Chiba (JP). 斉藤 晃 (SAITO, Hikaru) [JP/JP]; 〒112-0015 東京都文京

区目白台 1-9-4-308 Tokyo (JP). 中里 昇吾 (NAKAZATO, Shogo) [JP/JP]; 〒110-0004 東京都台東区下谷 2-19-5-202 Tokyo (JP). 奈良原 智明 (NARAHARA, Tomoaki) [JP/JP]; 〒167-0054 東京都杉並区松庵 1-3-16 Tokyo (JP). 吉川 治宏 (KIKKAWA, Haruhiro) [JP/JP]; 〒154-0022 東京都世田谷区梅丘 1-55-2 Tokyo (JP). 勝原 透匡 (KATSUHARA, Yukimasa) [JP/JP]; 〒135-0091 東京都港区台場 1-3-4-1502 Tokyo (JP). 荻 猛 (OGI, Takeshi) [JP/JP]; 〒156-0054 東京都世田谷区桜丘 5 丁目 7 番 1 1 号 Tokyo (JP).

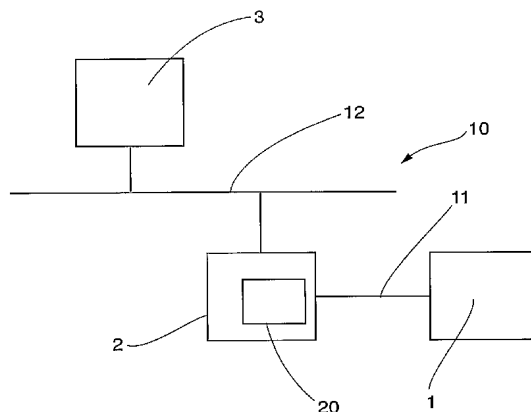
(74) 代理人: 市原 俊一, 外 (ICHIHARA, Shunichi et al.); 〒160-0004 東京都新宿区四谷 2 丁目 8 番地 コーポクロバ浜 505 号 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: PORTABLE PERSONAL SERVER WITH BIOLOGICAL INFORMATION RECOGNIZER

(54) 発明の名称: 生体情報認識装置を備えた携帯型パーソナルサーバ装置



(57) Abstract: A portable personal server (1) connectable through a network (11) with a PC (2) connected with an external network (12) and permits communication with the PC (2) only when user's fingerprint information read out by means of a fingerprint authentication unit (22) matches registered information. In order to communicate through the network (11), the portable personal server (1) and the PC (2) acquires an address using APIPA so that the collision of address does not take place in the external network (12). Consequently, the portable personal server (1) also functions as a network server on the external network (12). A portable personal server exhibiting high confidentiality of data and suitable for central management of data can thereby realized.

(57) 要約: 携帯型パーソナルサーバ装置 (1) は、外部ネットワーク (12) に接続された PC (2) にネットワーク (11) を介して接続可能であり、指紋認証装置 (22) により使用者の指紋情報を読み取り、登録情報と一致した場合のみ PC (2) との通信を許可する。携帯型パーソナルサーバ装置 (1) と PC (2) とは、ネットワーク (11) を介して通信するために、外部ネットワーク (12) とアドレスの衝突が起こらないよう APIPA を用いてアドレスを取得する。この結果、携帯型パーソナルサーバ装置 (1) は外部ネットワーク (12) 上のネットワークサーバとしても機能する。データの機密性が高く、データを一元管理するのに適した携帯型パーソナルサーバ装置を実現できる。



WO 2005/064485 A1



LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明細書

## 生体情報認識装置を備えた携帯型パーソナルサーバ装置

## 5 技術分野

本発明は、ネットワーク接続手段を備えた通信端末と通信することにより、当該通信端末のネットワーク接続手段によって接続されたネットワークとの間でデータ交換などの処理を行うことのできるサーバ機能を有する生体情報認識装置を備えた携帯型パーソナルサーバ装置に関するものである。

10

## 背景技術

ビジネスおよび日常で必要となる情報は、電子データとしてパーソナルコンピュータ（P C）の内部記憶装置、ネットワークに接続されたサーバシステム、あるいはP Cに対する外部接続記憶装置などに格納されている。そして、これらのデータ

15 へのアクセスおよびデータの処理にはP Cが広く一般的に使用されている。

近年、インターネットの普及により、あらゆる場所に設置されたP Cからネットワークを介して必要なデータにアクセスすることが可能になった。そのため、ユーザは、データが必要になった時に、傍にあるP Cを利用してネットワークに接続して、必要なデータにアクセスするようになっている。この結果、1人のユーザが、

20 オフィスに設置されているP C、出張など外出時に使用する携帯型P C、自宅に設置されているP Cなど、2、3台のP Cを使用することが一般的に行なわれている。一方で、オフィスや家庭に設置されたP Cを複数のユーザが共同で利用することも行なわれている。

また、情報への常時アクセスの必要性が高まるにつれ、P D Aや携帯電話といった情報処理端末へデータをコピーして常時携帯するといったことも行われている。単にデータを常時携帯するための手段としては、U S B トークン、メディアカードなどのストレージデバイスが用いられている。

25

ここで、P Cや情報処理端末へデータを無制限にコピーすることは情報の漏洩に直結する。したがって、データに対するアクセス権を識別するための手段として、パスワードや生体情報を用いた端末アクセス制御技術が用いられている。

- このような端末アクセス制御技術を有するP Cとしては、指紋認証カードをP C  
5 スロットに差込んだ後、自分自身のP Cとして使用するミニコンピュータが案出されている（例えば、特許文献1 参照。）。また、指紋センサを搭載することにより、本人認証およびセキュリティ機能を提供するP D Aが案出されている（例えば、特許文献2 参照。）。

〔特許文献1〕 特開平1 1－2 7 2 3 4 9号公報

- 10 〔特許文献2〕 米国特許第6 0 1 6 4 7 6号明細書

#### 発明の開示

（発明が解決しようとする課題）

- 1 人のユーザが複数のP Cを利用してネットワークを介してデータへのアクセス  
15 を行うようになった結果、アクセスしたデータが複数のP Cに分散して格納されてしまうことが頻繁に発生している。また、ユーザがアクセスしたデータに処理を施した場合には、処理前のデータと処理後のデータが異なるP Cに分散して保持されてしまい、一つの情報の一貫性が保持できない。

- そこで、ネットワークに接続されているサーバにデータを一元的に集めて保存、  
20 あるいは処理を行えば、比較的容易に情報の一貫性を保つことができる。この場合には、サーバをユーザ自身が管理することは容易ではないため、他人が管理するサーバに、当該サーバの能力および管理者を信頼して対価を支払ってデータを預けることになる。

- しかし、個々のユーザ自身だけがアクセスすればよい個人データを、物理的に離  
25 れており、かつ、自らの管理下でないサーバに預けることは不安であり、コストもかかる。また、ネットワークに接続されているサーバは通常多数のユーザによって共有されている。したがって、どのような安全手段を施したとしても、必然的に当

該サーバにアクセス可能な他人に情報が漏洩する危険性が高い。また、ネットワークへのアクセスが不可能な場合には、当該サーバへのアクセスができず、必要なデータを必要な時に取得することが不可能になってしまう。

また、P Cを複数のユーザで共有する場合には、ユーザ同士が物理的に同じ記憶  
5 装置にデータを保存するために、P Cを共有する他のユーザに対してデータが漏洩する危険性が高い。

情報処理端末でデータを携帯する場合には、情報処理端末の操作性が、一般的にP Cより劣り、汎用性も低いので、通常はP Cを主端末として用いて情報処理端末は補助端末として用いている。この結果、ユーザは主端末であるP Cと補助端末で  
10 ある情報処理端末との間のデータフォーマットの変換、データの一貫性の維持などに悩まされる。

携帯型の記憶媒体、例えばストレージデバイスでデータを携帯する場合には、ネットワークに接続されたサーバや、その他のネットワーク機器は、当該ストレージ  
15 レジデバイスと直接通信を行うことが出来ない。したがって、ユーザは一旦P Cにストレージデバイスに格納されたデータを移動し、その後、P Cからネットワークにデータを送信するといった煩雑な操作をすることとなる。この結果、P Cにデータのコピーが残ってしまう場合があり、情報が漏洩する危険性がある。

一方、認証用デバイスによりP Cを自分自身のP Cとして使用する場合には、認証用のデバイスは、単に認証情報をP Cに流し、P C上の指定されたサービスを起  
20 動するために用いられている。また、これら認証用デバイスから提供されるサービスは通常固定されており、専用C P Uを搭載するものではアップデートが可能とされている。しかし、その場合でも数百キロバイト程度の非常に限定的なサービス書き込みエリアしか提供されていない。また、メーカー独自のA P Iを使ってプログラミングをする必要がある等、これら認証用デバイスが提供するサービスは実質的  
25 にはメーカー側が提供するサービスに限定されているのが現状であり、拡張性が乏しい。

次に、企業の秘密データなどを企業が従業員と交換する場合には、企業のシステ

ム担当者は自社ネットワーク内におけるデータの移動、処理に関しては、当該担当者の管理ポリシーに従って管理することが出来る。しかし、一旦自社ネットワークの外部に移動したデータについては管理ポリシーを徹底させることは困難である。例えば、従業員が自宅に設置されたPCを用いてアクセスし、取得した情報について社内5 内の管理ポリシーを適用することは難しく、従業員の良識に依存するしかない。

本発明の課題は、このような点に鑑みて、データを一元的に管理するために、ネットワーク接続手段を備えた通信端末と通信することにより、当該通信端末のネットワーク接続手段によって接続されたネットワークとの間でデータの処理が可能なサーバ機能を有する携帯型パーソナルサーバ装置を提案することにある。

10

(課題を解決するための手段)

上記の課題を解決するために、本発明の携帯型パーソナルサーバ装置は、

ネットワーク接続手段を備えた通信端末との間でデータ処理を行うローカルサーバ手段と、

15 前記通信端末のネットワーク接続機能によって当該通信端末に接続されたネットワークとの間で、データ処理を行うネットワークサーバ手段と、

生体情報に基づき個人認証を行う個人認証手段と、

前記個人認証手段により認証された場合にのみ、前記ローカルサーバ手段および前記ネットワークサーバ手段を利用可能にする制御手段とを有していることを特徴20 としている。

本発明の携帯型パーソナルサーバ装置は、ネットワーク接続手段を備えた通信端末との間でデータ処理を行うローカルサーバ手段を有している。すなわち、PCなどのネットワーク接続手段を備えた通信端末と通信することによりローカルサーバとして機能するので、あらゆる場所に設置されているPCを用いて携帯型パーソナルサーバ装置に格納されたデータにアクセスすることができる。さらに、PCにより25 データ処理を施した場合でも、処理後のデータを常に携帯型パーソナルサーバ装置に保存して最新のデータに更新することができる。その結果、複数のPCにデー

タが散在することはなくデータの一貫性が保たれる。データのフォーマットを気にする必要もない。また、複数のPCにデータが散在することがないので携帯型パーソナルサーバ装置の管理を徹底することにより、企業等の管理ポリシーに従ってデータを管理することができる。

- 5      また、本発明の携帯型パーソナルサーバ装置は、通信端末に接続されたネットワークとの間でデータの処理を行うネットワークサーバ手段を有している。従って、携帯型パーソナルサーバ装置からネットワークに向けて情報を発信することができ、ネットワークからのデータを受け取り、自動処理を行い、指定された通信端末装置に向けて処理結果を返すといった動作も可能である。また、携帯型パーソナルサーバ装置は、通信端末を介してネットワークに接続されているが、携帯型パーソナルサーバ装置自体がネットワークサーバ機能を有しているので、当該通信端末に一時的であってもデータが保存されることがない。このため、当該通信端末に保存されたデータから情報が漏洩してしまうことがない。
- 10

- さらに、本発明の携帯型パーソナルサーバ装置は、指紋などの生体情報に基づき個人認証を行う個人認証手段と、この個人認証手段により認証された場合にのみ、前記ローカルサーバ手段および前記ネットワーク手段を利用可能にする制御手段とを有している。したがって、持ち主以外は携帯型パーソナルサーバ装置に蓄積されたデータにアクセスすることができない。このため、携帯型パーソナルサーバ装置を紛失した場合でも、他者へのデータの漏洩を避けることができる。特に、携帯型
- 20      パーソナルサーバ装置は一切の操作の入出力装置（キーボード、ディスプレイなどの装置）を持たない構成とすることができる。このようにすれば、携帯型パーソナルサーバ装置を紛失した場合において、他人が内部データにアクセスすることが困難であり、機密性が高い。

- また、個人認証手段により携帯型パーソナルサーバ装置の持ち主を特定した上で、固有の電子証明書などを利用したネットワーク認証手段によって携帯型パーソナルサーバ装置をネットワークサーバとして機能させる。この結果、ネットワークからネットワークサーバとして機能している携帯型パーソナルサーバ装置へアクセスし
- 25

ようとする他人は、当該携帯型パーソナルサーバ装置が間違いなく当該携帯型サーバの持ち主のものであることを確認できる。また、当該携帯型サーバの持ち主本人が携帯型パーソナルサーバ装置を使用中であることも確認できるので、悪意のある者によって運用されたネットワークサーバへアクセスする危険性を減らすことができる。さらに、仮に携帯型パーソナルサーバ装置へアクセス中に問題が発生した場合、問題の発生原因が当該携帯型パーソナルサーバ装置および持ち主に起因するものであると特定することができるので、通信システムの信頼性を確保できる。

ここで、個人認証手段は、指紋センサなどの生体情報認識装置を備え、当該生体情報認識装置により読み込まれた読込生体情報が予め登録されている登録生体情報に一致するか否かにより個人認証を行うように構成することができる。

また、本発明の携帯型パーソナルサーバ装置は、格納データを前記読込生体情報を用いて暗号化するデータ暗号化手段を有していることが望ましい。持ち主の生体情報に基づいて携帯型パーソナルサーバ装置に格納されるデータが暗号化されているので、携帯型パーソナルサーバ装置を分解して内部のデータにアクセスしようとした場合でも、格納されているデータを他人が解読することは困難あり、他人へのデータの漏洩を避けることができる。

さらに、本発明の携帯型パーソナルサーバ装置は、前記読込生体情報が前記登録生体情報に一致した場合に、前記読込生体情報に基づいて公開鍵暗号方式に用いられる鍵の生成と保管を行い、当該鍵を用いて送信されるデータを暗号化する通信暗号化手段を有していることが望ましい。通信暗号化手段により、ネットワークを介してデータの送受を行なう場合のデータが保護されるので、通信システムのセキュリティが確保される。

さらにまた、本発明の携帯型パーソナルサーバ装置は、前記通信端末に接続するための通信ケーブル端子を有しており、この通信ケーブル端子を介して前記通信端末から電源の供給を受けるようになっていることが望ましい。電源がP Cなどの通信端末の側から供給されるので、携帯型パーソナルサーバ装置は自己電源を持つ必要がない。この結果、携帯型パーソナルサーバ装置を小型で安価に製造することが



できるので、個々のユーザが常時携帯するのに便利である。また充電等の必要もない。さらに、物理的な手段で携帯型パーソナルサーバ装置と通信端末を通信可能に接続するので携帯型パーソナルサーバ装置と通信端末との間の通信を盗聴される危険性が少ない。

- 5 この場合、前記通信ケーブル端子をUSB接続端子とすることが望ましい。

#### 図面の簡単な説明

図1は、本発明の携帯型パーソナルサーバ装置を用いて構築した通信システムの一例を示す全体構成図である。

- 10 図2は、図1の携帯型パーソナルサーバ装置のシステム構成図である。

図3は、図1の携帯型パーソナルサーバ装置の外観斜視図である。

図4は、図1の携帯型パーソナルサーバ装置のソフトウェア構成を表す概念図である。

#### (符号の説明)

- 15 1 携帯型パーソナルサーバ装置  
2 PC  
3 外部サーバ  
10 通信システム  
11 ネットワーク  
20 12 外部ネットワーク  
20 20 リレーサービス  
21 CPU  
22 指紋認証装置  
23 通信インタフェース  
25 23a 接続端子  
24 メモリ  
25 25 ストレージメディアカードスロット

26 フラッシュROM

27 指紋センサ部分

28 USBケーブル

31 装置本体

5 41 オペレーティングシステム

42 指紋認証プログラム

43 サーバプログラム

44 暗号プログラム

## 10 発明を実施するための最良の形態

### (全体構成)

図1は、本発明を適用した通信システムの一例を示す全体構成図である。図1に示すように、本形態の通信システム10は、携帯型パーソナルサーバ装置1と、ネットワーク接続手段を備えたPC2とを有しており、携帯型パーソナルサーバ装置1とPC2とはネットワーク11により通信可能に接続されている。PC2はインターネットなどの外部ネットワーク12に接続されている。ネットワーク11および外部ネットワーク12はいずれもIEEE802ネットワークであり、TCP/IPで接続されている。外部ネットワーク12には外部サーバ3が接続されている。

## 20 (携帯型パーソナルサーバ装置の構成)

図2は携帯型パーソナルサーバ装置のシステム構成図である。携帯型パーソナルサーバ装置1は、CPU21、指紋認証装置22、通信インタフェース23、メモリ(RAM)24、ストレージメディアカードスロット25、フラッシュROM26を有している。フラッシュROM26には、オペレーティングシステム(OS)41、指紋認証プログラム42、サーバプログラム43、暗号プログラム44が記憶されている。

図3は携帯型パーソナルサーバ装置の外観斜視図である。携帯型パーソナルサー

バ装置 1 は、手のひら大の大きさの卵形の輪郭形状をした装置本体 3 1 を備え、装置本体 3 1 の表面中央部分には指紋認証装置 2 2 の指紋センサ部分 2 7 が配置されている。装置本体 3 1 の先端部には通信インタフェース 2 3 の接続端子 2 3 a が配置されている。通信インタフェース 2 3 は U S B 通信インタフェースであり、接続  
5 端子 2 3 a には、ネットワーク 1 1 に接続する U S B ケーブル 2 8 が接続されている。

ここで、通信インタフェース 2 3 は、パーソナルサーバ装置 1 と P C 2 とがネットワーク 1 1 を介して通信する機能、および、パーソナルサーバ装置 1 が P C 2 を介して外部ネットワーク 1 2 と通信する機能を提供する。また、指紋認証装置 2 2  
10 と指紋認証プログラム 4 2 は個人認証手段を提供する。すなわち、指紋認証装置 2 2 は指紋センサ部分 2 7 で検出した使用者の指紋情報を読み取り、指紋認証プログラム 4 2 は、読み取った指紋情報を予め登録された指紋情報と照合する。指紋情報が一致した場合には使用者が予め登録された使用者、本人であることが認証される。

サーバプログラム 4 3 は、P C 2 との間でデータの処理を行うローカルサーバ機能と、外部ネットワーク 1 2 との間でデータの処理を行うネットワークサーバ機能  
15 とを提供する。暗号プログラム 4 4 は、指紋情報に基づいてパーソナルサーバ装置 1 に格納されるデータを暗号化するデータ暗号化手段を提供する。

図 4 はパーソナルサーバ装置のソフトウェア構成を表す概念図である。ハードウェアに、下層から O S、データベース、データプロバイダインタフェース、フレームワーク、サービスプロバイダインタフェース、サービス、メッセージング A P I  
20 が構成されている。

#### (携帯型パーソナルサーバ装置と通信端末との接続)

携帯型パーソナルサーバ装置 1 は、通信インタフェース 2 3 によって P C 2 と接続  
25 されることにより、P C 側から電源が供給されて起動する。使用者は、指紋認証装置 2 2 の指紋センサ部分 2 7 に指先をあてて、指紋情報による個人認証を受ける。指紋認証装置 2 2 が取得した読込指紋情報が予めパーソナルサーバ装置 1 に登録さ

れている登録指紋情報と一致した場合には、携帯型パーソナルサーバ装置 1 はネットワーク 1 1 を介して P C 2 と通信可能になる。

携帯型パーソナルサーバ装置 1 と P C 2 は、ネットワーク 1 1 を介して通信可能にするために、APIPA を用いてアドレスを取得する。この際、P C 2 に接続された  
5 外部ネットワーク 1 2 とアドレスの衝突が起こらないよう協調してアドレッシングが行なわれる。P C 2 は、アドレッシングの後、W i n d o w s（登録商標）等の P C に実装されているリレーサービス 2 0 を用いてディスカバリを行い、パーソナルサーバ装置 1 を発見する。ディスカバリを含め、携帯型パーソナルサーバ装置 1 と P C 2 との間のコミュニケーションには S O A P（Simple Object Access  
10 Protocol）というプロトコルが利用される。その表現言語としては、XML が用いられる。

P C 2 から携帯型パーソナルサーバ装置 1 が発見されると、外部ネットワーク 1 2 と携帯型パーソナルサーバ装置 1 は通信することが可能になる。携帯型パーソナルサーバ装置 1 は、さらに、ネットワーク認証手段により、外部ネットワーク 1 2  
15 に対して固有の電子証明書を用いた接続作業を行う。この作業の結果、外部ネットワーク 1 2 と携帯型パーソナルサーバ装置 1 との接続が確立されると、携帯型パーソナルサーバ装置 1 は外部ネットワーク 1 2 上のネットワークサーバとして機能する。ネットワーク認証手段によって、外部ネットワーク 1 2 からネットワークサーバとして機能している携帯型パーソナルサーバ装置 1 へアクセスしようとする他人  
20 や外部サーバ 3 は、携帯型パーソナルサーバ装置 1 が間違いなく当該携帯型パーソナルサーバ装置 1 の予め登録された使用者のものであることを確認できる。

ここで、P C 2 のリレーサービス 2 0 は、P C 2 上のアプリケーションから携帯型パーソナルサーバ装置 1、携帯型パーソナルサーバ装置 1 から P C 2 上のアプリケーション、または携帯型パーソナルサーバ装置 1 から外部サーバ 3 等への S O A  
25 P メッセージをリレーする。また、携帯型パーソナルサーバ装置 1 は、指紋認証装置 2 2 で得た指紋情報をもとに公開鍵暗号方式に用いられる鍵の生成およびその保管を行う。また、必要に応じて共通鍵の生成をおこない、共通鍵、公開鍵の両方を

用いた通信暗号化の機能を提供する。

(作用効果)

使用者が携帯型パーソナルサーバ装置 1 を携帯することにより、常にデータとアプリケーションを当該携帯型パーソナルサーバ装置 1 に格納することができる。したがって、データを一元的に管理でき、特定のアプリケーションについて、PC 自体にインストールすることなく、複数の PC から使用することが可能となる。

また、携帯型パーソナルサーバ装置 1 は、指紋情報による個人認証手段を有しているので、登録された持ち主以外は PC 2 と接続してローカルサーバあるいはネットワークサーバとして動作させることができない。加えて、携帯型パーソナルサーバ装置 1 は固有の入出力装置も持たないので、持ち主本人以外は、格納されているデータにアクセスすることが難しく、情報の漏洩の危険がない。また、外部ネットワーク 12 からネットワークサーバとして機能している携帯型パーソナルサーバ装置 1 へアクセスしようとする他人は、当該携帯型パーソナルサーバ装置 1 が間違いなく当該携帯型パーソナルサーバ装置 1 の予め登録された使用者のものであることを特定することができるので、通信システム 10 の信頼性が高い。

さらに、携帯型パーソナルサーバ装置 1 は、通信システム 10 において、TCP / IP で PC 2 および外部ネットワーク 12 と接続されてローカルサーバおよびネットワークサーバとして機能する。したがって、一般的なインターネット用ブラウザを用いて、相互動作が可能な形でユーザインタフェースを提供することができる。また、外部ネットワーク 12 に接続されている外部サーバ 3 にデータやメッセージを受け渡して、外部サーバ 3 にあるプログラムを直接利用することができる。

さらにまた、携帯型パーソナルサーバ装置 1 と外部ネットワーク 12 との接続には、PC 2 に実装されているリレーサービス 20 を利用するだけなので、PC 2 にデータが一時的にも保管されることがない。したがって、PC 2 から情報が漏洩する危険性がない。

次に、携帯型パーソナルサーバ装置 1 は、一般の認証用デバイスやストレージデ

バイスと異なり、通常のサーバハードウェアと同様に、CPU 21、フラッシュROM 26、RAM 24などから成るハードウェア構成を取っているため、内部のソフトウェア構成として標準的なアプリケーションサーバと同様の構成を採用することができる。また、固有のCPU 21を有しているため、PC 2に負荷をかけるこ  
5 となく、携帯型パーソナルサーバ装置1内部のサービスを提供し、外部からの計算要求を処理し、自動的に計算処理結果を出力するといった通信システムを構築できる。

また、携帯型パーソナルサーバ装置1内部のサービスを提供するに当り、特殊なAPIを使うのではなく、例えばW3Cにおいて定義されている標準的なWeb  
10 Servicesの仕様に基づいたAPIとして提供することが出来るので、サービス開発者は新たなプログラミング言語を学ぶ必要性がなく、携帯型パーソナルサーバ装置1の提供するサービスを使ったアプリケーションの開発、あるいはサービス自体の機能拡張作業等が容易である。

さらに、携帯型パーソナルサーバ装置1はXML/ SOAPに対応し、固有のデータベースを保有するため、一般的なデータ通信システムとして用いることができる。また、開発したアプリケーションの汎用性が高い。また、携帯型パーソナルサーバ装置1は、ストレージメディアカードスロット25を備えているので、必要に応じてメディアカードを入れ替えることにより、理論上無限大のストレージスペースを提供することが出来る。この場合でも、暗号プログラム44は、指紋情報に基  
20 づいてメディアカードに格納されるデータを暗号化するので、データの機密性が高い。

さらにまた、携帯型パーソナルサーバ装置1とPC 2とを接続する通信インタフェース23としてUSBを用いているので、携帯型パーソナルサーバ装置1にPC  
2から電源を供給することができる。したがって、自己電源を持つ必要がなく装置  
25 の小型化が図れる。また、充電等の必要もないので携帯に便利である。

(その他の実施の形態)

なお、上記の携帯型パーソナルサーバ装置 1 では、P C 2 との接続に U S B を使用している。P C との間の物理的接続形態は無線、有線を問わず、例えば、イーサネット、B l u e t o o t h、W L A N、赤外線などが利用可能である。いずれの場合にも、S S L 通信などを用いてデータを全て暗号化することにより、通信のセ  
5 キュリティを確保できる。

#### 産業上の利用の可能性

本発明によれば、ユーザが携帯型パーソナルサーバ装置を携帯できるので、常にデータとアプリケーションを一元的に管理することができる。また、P C などのネットワーク接続手段を備えた通信端末と通信することによりローカルサーバ、ネットワークサーバとして機能するので、あらゆる場所に設置されている P C を用いて、  
10 携帯型パーソナルサーバ装置に格納されたデータとアプリケーションにアクセスすることができる。さらに、指紋センサなどの生体情報による個人認証手段を備えているので、持ち主以外は携帯型パーソナルサーバ装置をサーバ装置として機能させることができない。したがって、携帯型パーソナルサーバ装置を紛失した場合でも、  
15 格納されているデータに他人がアクセスすることはできないので、データの漏洩を避けることができる。また、ネットワークから携帯型パーソナルサーバ装置にアクセスしようとする他人は、そのネットワークサーバとして機能する携帯型パーソナルサーバ装置が常に持ち主本人のものであることを認識することができるので、通  
20 信の信頼性を確保することができる。

したがって、本発明の携帯型パーソナルサーバ装置を用いれば、分散型のネットワークサーバを用いたネットワークアプリケーションを利用する場合などにおいて、信頼性の高い通信システムを構築できる。

## 請求の範囲

1. ネットワーク接続手段を備えた通信端末との間でデータ処理を行うローカルサーバ手段と、

- 5 前記通信端末のネットワーク接続機能によって当該通信端末に接続されたネットワークとの間で、データ処理を行うネットワークサーバ手段と、  
生体情報に基づき個人認証を行う個人認証手段と、  
前記個人認証手段により認証された場合にのみ、前記ローカルサーバ手段および  
前記ネットワーク手段を利用可能にする制御手段とを有している携帯型パーソナル  
10 サーバ装置。

2. 請求項 1 において、

- 前記個人認証手段は指紋センサなどの生体情報認識装置を備え、当該生体情報認識装置により読み込まれた読込生体情報が予め登録されている登録生体情報に一致  
15 するか否かにより個人認証を行う携帯型パーソナルサーバ装置。

3. 請求項 2 において、

格納データを前記読込生体情報を用いてデータを暗号化するデータ暗号化手段を有している携帯型パーソナルサーバ装置。

20

4. 請求項 2 において、

前記読込生体情報が前記登録生体情報に一致した場合に、前記読込生体情報に基づいて公開鍵暗号方式に用いられる鍵の生成と保管を行い、当該鍵を用いて送信されるデータを暗号化する通信暗号化手段を有している携帯型パーソナルサーバ装置。

25

5. 請求項 1 ないし 4 のうちのいずれかの項において、

前記通信端末に接続するための通信ケーブルを有しており、



前記通信ケーブルを介して前記通信端末から電源の供給を受ける携帯型パーソナルサーバ装置。

6. 請求項5において、

5 前記通信ケーブルはU S Bである携帯型パーソナルサーバ装置。

図 1

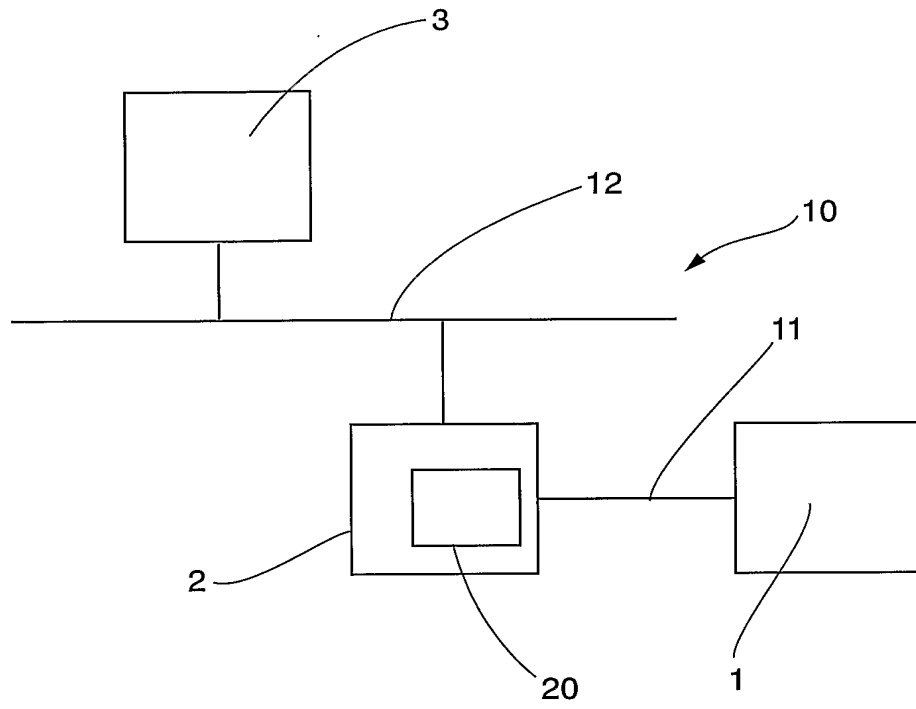


図 2

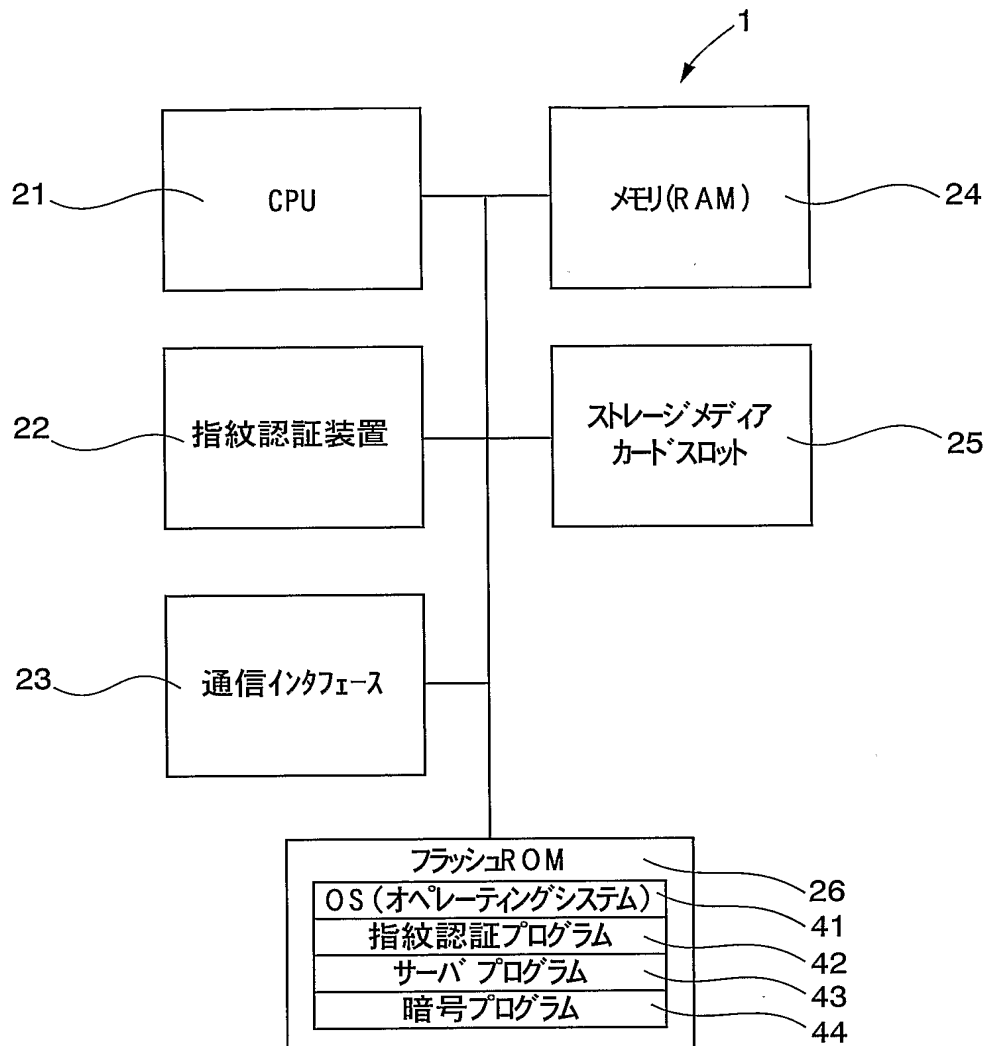


図 3

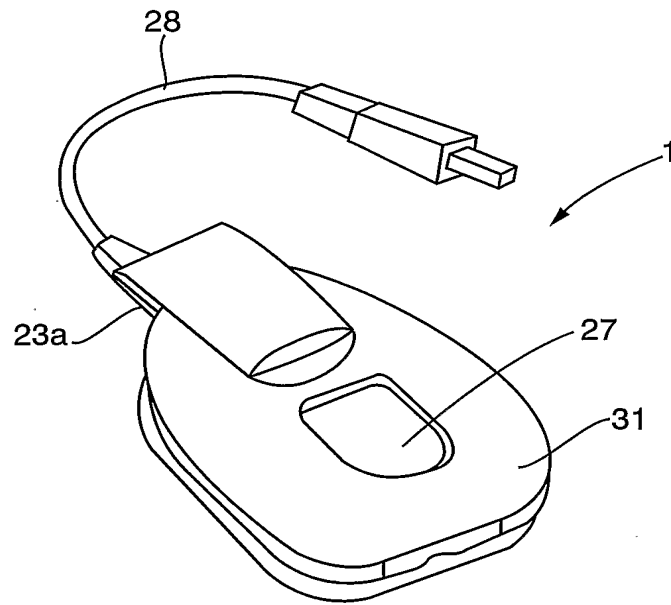
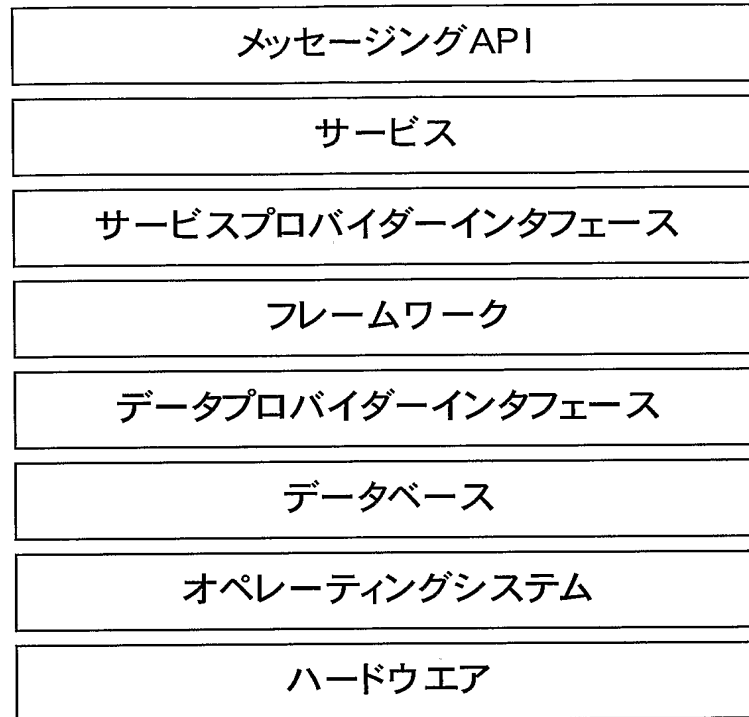


図 4



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/16815

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F15/00, G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F15/00, G06F1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-123437 A (Fujitsu Ltd.), 26 April, 2002 (26.04.02), Full text; all drawings (Family: none)	1-6
A	JP 2001-358828 A (Masahiko OKUNO), 26 December, 2001 (26.12.01), Full text; all drawings (Family: none)	1-6
A	JP 10-260749 A (Sun Micro Systems Inc.), 29 September, 1998 (29.09.98), Full text; all drawings & EP 853413 A2 & CN 1190215 A & SG 77151 A	1-6

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
06 April, 2004 (06.04.04)

Date of mailing of the international search report  
20 April, 2004 (20.04.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/JP03/16815

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-316818 A (TRW Inc.), 16 November, 1999 (16.11.99), Full text; all drawings & EP 924657 A2 & US 6038666 A	1-6
A	JP 2001-92668 A (Sony Corp.), 06 April, 2001 (06.04.01), Full text; all drawings (Family: none)	1-6

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl<sup>7</sup> G06F15/00, G06F1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl<sup>7</sup> G06F15/00, G06F1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926年-1996年

日本国公開実用新案公報 1971年-2004年

日本国実用新案登録公報 1996年-2004年

日本国登録実用新案公報 1994年-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-123437 A (富士通株式会社) 2002.04.26, 全文, 全図 (ファミリーなし)	1-6
A	JP 2001-358828 A (奥野 昌彦) 2001.12.26, 全文, 全図 (ファミリーなし)	1-6
A	JP 10-260749 A (サンマイクロシステムズ インコーポレーテッド) 1998.09.29, 全文, 全図 & EP 853413 A2 & CN 1190215 A & SG 77151 A	1-6

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

06.04.2004

国際調査報告の発送日

20.4.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

漆原 孝治

5B

9366

電話番号 03-3581-1101 内線 3546



C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-316818 A (ディーアールダブリュー・インコーポレーテッド) 1999.11.16, 全文, 全図 & EP 924657 A2 & US 6038666 A	1-6
A	JP 2001-92668 A (ソニー株式会社) 2001.04.06, 全文, 全図 (ファミリーなし)	1-6